B1

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Patentschrift**

(10) **DE 40 15 482 C 1**

(51) Int. Cl.[5]:
G 06 F 12/14
G 07 C 9/00

(21) Aktenzeichen: P 40 15 482.3-53
(22) Anmeldetag: 14. 5. 90
(43) Offenlegungstag: —
(45) Veröffentlichungstag der Patenterteilung: 25. 7. 91

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

(73) Patentinhaber:
Competence Center Informatik GmbH, 4470 Meppen, DE

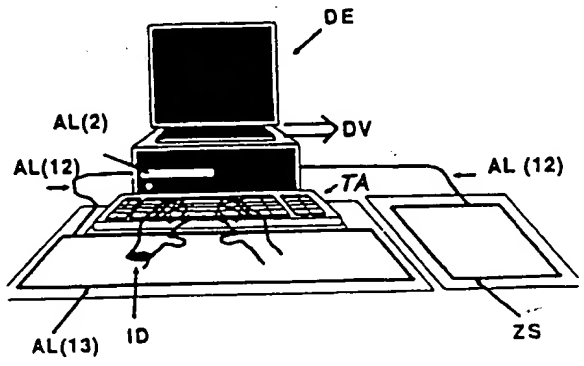
(74) Vertreter:
Pagenberg, J., Dr.jur.; Frohwitter, B., Dipl.-Ing., Rechtsanwälte; Geißler, B., Dipl.-Phys.Dr.jur., Pat.- u. Rechtsanw.; Bardehle, H., Dipl.-Ing.; Dost, W., Dipl.-Chem. Dr.rer.nat.; Altenburg, U., Dipl.-Phys., Pat.-Anwälte, 8000 München

(72) Erfinder:
Holzapfel, Stephan, 4470 Meppen, DE; Book, Nobert, 4530 Ibbenbüren, DE; Kraaibeek, Peter, 4450 Lingen, DE

(56) Für die Beurteilung der Patentfähigkeit in Betracht gezogene Druckschriften:
US-Z, IBM Technical Disclosure Bulletin, Vol. 31, No. 9, Februar 1989, S. 223;
DE-Z, Funkschau 13/1986, S. 24-28, Firmenschrift der Unina, Unises, a revolutionary 100% watertightsecurrty system for your PC;

(54) System zur berührungslosen Authentisierung des Nutzers einer Datenendeinrichtung eines Datenverarbeitungssystems

(57) Es wird ein System zur berührungslosen Authentisierung des Nutzers einer Datenendeinrichtung eines Datenverarbeitungssystems angegeben. Der Nutzer trägt, schwer verlierbar, einen Identifikationsträger mit sich, der innerhalb einer Entfernung von weniger als 1 m abgefragt werden kann. Ein Abstandsleser, der nahe bei der Datenendeinrichtung angebracht und über ein Verbindungskabel mit ihr verbunden ist, fragt kontinuierlich die persönliche Nutzerkennung auf dem Identifikationsträger ab. Wenn die vorbestimmte Entfernung für vorbestimmte Zeitspannen überschritten wird, so wird die Datenendeinrichtung teilweise oder ganz blockiert. Ein Schreibgerät programmiert den Identifikationsträger zu vorgegebenen Zeitpunkten, an denen der Nutzer anderweitig identifiziert wird. Das Schreibgerät übermittelt die erzeugte Nutzerkennung an das Datenverarbeitungssystem. Sowohl bei der Abfrage als auch bei der Programmierung der persönlichen Nutzerkennung befindet sich der Identifikationsträger in einem magnetischen Wechselfeld.



Beschreibung

Die Erfindung bezieht sich auf ein System zur Authentisierung des Nutzers einer Dateneinrichtung eines Datenverarbeitungssystems, wie es im Oberbegriff des Patentanspruchs 1 angegeben ist. Ein derartiges System ist aus einer Firmenschrift der Firma UNINA bekannt, in welcher das Sicherheitssystem UNISES beschrieben ist. Die Erfindung bezieht sich ferner auf ein System zur Authentisierung nach dem Oberbegriff des Patentanspruchs 13.

Um gefährdete oder anderweitig schutzwürdige Datenverarbeitungssysteme vor unberechtigtem Zugriff zu schützen, werden üblicherweise sogenannte LOGON-Verfahren eingesetzt. Hierzu werden an einer Datenendeinrichtung des Datenverarbeitungssystems Nutzerkennungen und Paßwörter eingegeben, die dem autorisierten Nutzer und dem System bekannt sind. Das System identifiziert den Nutzer anhand seines Paßworts und gewährt ihm an der benutzten Datenendeinrichtung die zugewiesenen Zugriffsrechte.

Dieses Verfahren weist Schwächen auf, durch welche ein Paßwort verhältnismäßig leicht umgangen werden kann:

- Simple Paßworte sind leicht aufdeckbar; der Schutz des Systems vor unberechtigten Nutzern ist nicht gewährleistet.
- Wirksame und damit lange Paßworte werden vom autorisierten Nutzer leicht vergessen. Daher werden diese häufig schriftlich aufgezeichnet und können ebenfalls aufgedeckt werden.
- Nutzern, die ihr Identifikationsmerkmal "Paßwort" vergessen haben, stehen die Systemleistungen in kritischen Situationen nicht zur Verfügung.
- Der Vorgang des LOGON belastet den Nutzer zeitlich und lenkt ihn von der eigentlichen Nutzung des Systems ab.
- Paßworte können bei der Eingabe über die Tastatur durch Beobachten der Finger ausgespäht werden.

Die aufgeführten Unzulänglichkeiten machen die autorisierte Nutzung des Datenverarbeitungssystems unbequem. Hieraus resultiert häufig die eingeschränkte oder unzulängliche Nutzung der verfügbaren Sicherheitsmechanismen.

Die vorhandenen Sicherheitsmängel haben zu Überlegungen geführt, wie die Datensicherheit bei Benutzung einer Dateneinrichtung grundsätzlich verbessert werden könnte. Das eingangs erwähnte Sicherheitssystem UNISES verzichtet auf die manuelle Eingabe von Paßwörtern und authentisiert den Nutzer eines Personal-Computers automatisch. Die Vorrichtung besteht aus einem integrierten Schaltkreis, der im Personal-Computer eingebaut und mit leistungsfähigen Verschlüsselungsfunktionen versehen ist, sowie aus einem kleinen Hochfrequenzsender, der in einer Tasche des Nutzers getragen wird und eine persönliche Kennung aktiv abstrahlt. Der Hochfrequenzsender hat eine Reichweite von 5 Metern und die Funkverbindung selbst ist bereits durch Verschlüsselungsalgorithmen geschützt. Wenn der Personal-Computer einen berechtigten Nutzer identifiziert, dann wird die Kennung aus dem Identifikationsträger in den Verschlüsselungs-Chip übertragen und es stehen außer den Standardfunktionen des Personal-Computers auch die geschützten Datenbereiche zur Verfügung. Die Authentisierung wird

kontinuierlich wiederholt. Wenn der Benutzer seinen Arbeitsplatz verläßt, dann führt der Personal-Computer die normale Datenverarbeitung fort; jedoch sperrt er jeden Zugang zu den Eingabegeräten (beispielsweise zu der Tastatur).

Dieses Autorisierungsverfahren erfüllt bereits einige der Bedingungen, die an einen verbesserten Datenschutz zu stellen sind. Insbesondere wird die Unterscheidung zwischen autorisierten und nicht-autorisierten Personen möglich, ohne daß der zugangsberechtigte Nutzer umständliche und zeitraubende Eingabeprozeduren vornehmen muß. Wenn sich der autorisierte Nutzer entfernt, wird der Personal-Computer automatisch in seinen sicherheitsempfindlichen Funktionen blokkiert. Nachteilig an dem bekannten Verfahren ist der aktive, d. h. batteriebetriebene und daher nicht wartungsfreie, sowie vergleichsweise voluminöse Sender. Nachteilig ist ferner, daß das unbekannte Verfahren nicht offen ist für weitere Authentisierungsschritte, die um so wichtiger werden, je größer das Datenverarbeitungssystem ist, an welches die Datenendeinrichtung angeschlossen ist.

Aus dem IBM Technical Disclosure Bulletin, Februar 1989, S. 223 und aus Funkschau 13/1986, S. 24—29 sind kleine, passive Identifikationsträger bekannt.

Die Erfindung hat sich die Aufgabe gestellt, bei einem berührungslosen Autentisierungsverfahren der vorausgesetzten Art den Schutz der persönlichen Nutzerkennung gegen Verlust oder Ausspähung weiter zu verbessern. Diese Aufgabe wird durch die kennzeichnenden Merkmale des Anspruchs 1 in Verbindung mit den Gattungsmerkmalen gelöst. Eine nebengeordnete Ausprägung des Erfindungsgedankens ist im Anspruch 13 angegeben.

Der erfindungsgemäße Identifikationsträger ist passiv, wartungsfrei und nicht größer als 3 × 15 × 20 mm. Bei dem erfindungsgemäßen System kann die Nutzerkennung auf dem Identifikationsträger häufig, zum Beispiel täglich, gewechselt werden. Hierzu werden die Nutzerkennungen von einer Stelle ausgegeben, die den Nutzer täglich auf Grund anderer Merkmale eindeutig identifiziert. Die neue Nutzerkennung wird dabei von einem an der ausgebenden Stelle installierten Schreibgerät erzeugt und in Verbindung mit der persönlichen Autentisierung durch die ausgebende Stelle automatisch an das System übermittelt. Das Schreibgerät kann mit einem der Abstandsleser kombiniert sein, der die Kennung aus dem Identifikationsträger ausliest und an die Datenendeinrichtung weitergibt.

Für die tägliche Autentisierung des Nutzers bei Übernahme der Kennung können biometrische Identifikationsverfahren zum Einsatz kommen, die zu kostenträchtig wären, wenn sie für jede Datenendeinrichtung eingesetzt würden. Beispielsweise kann die biometrische Identifikation eine automatische Auswertung der Unterschrift sein. In einem typischen Anwendungsbeispiel betritt ein Datenverarbeitungsnutzer das Betriebsgebäude seiner Firma und weist sich am Eingang durch Unterschrift aus. Statt einer automatischen Auswertung der Unterschrift kommt auch eine persönliche Identifizierung in Betracht. Er erhält daraufhin einen Identifikationsträger oder, falls er einen solchen schon besitzt, eine neue Kennung zur Nutzung des hausinternen Datenverarbeitungssystems. Die Kennung wird von einem Schreibgerät einprogrammiert und zusammen mit der Identität des Nutzers an das Datenverarbeitungssystem gemeldet. Das System gibt die Tageskennung dieses Nutzers gegebenenfalls an zusätzlich zu nutzende Sub-

systeme weiter.

Die Identifikationsträger ist mit dem Nutzer schwer verlierbar in der Nähe des Handgelenks verbunden. Beispielsweise kann der Identifikationsträger an einem Armband festgeklammert werden; er kann aber auch in eine Uhr, einen Armreif oder sogar einen Fingerring fest eingelassen sein. Nach der Übernahme des Identifikationsträgers oder der neuen Kennung begibt sich der Nutzer an seinen Arbeitsplatz. Die Datenendeinrichtung erkennt den Nutzer anhand der Kennung im Identifikationsträger. Hierzu ist in der Datenendeinrichtung ein Abstandsleser eingebaut, der jeden Nutzer in der Nähe der Datenendeinrichtung eindeutig identifiziert. Der Abstandsleser wird von einem speziellen Programm gesteuert, welches für den identifizierten Nutzer sofort und automatisch den LOGON-Vorgang über die Datenendeinrichtung auslöst. Der Nutzer kann ohne Verzögerung mit seiner Tätigkeit im Datenverarbeitungssystem beginnen. Der LOGON-Vorgang kann in den Fällen, in denen ein vollautomatischer Ablauf nicht sinnvoll ist, zusätzlich vom Nutzer aktiv angestoßen werden. Der Ablauf des LOGON wird an der Datenendeinrichtung angezeigt.

Bei der Kommunikation zwischen Datenendeinrichtung und Rechner können während des LOGON kryptographische Verfahren zum Einsatz kommen, die ein Aufdecken der Nutzerkennung durch Abhören von Leitungen erschweren.

Die Authentisierung des an der Datenendeinrichtung tätigen Nutzers wird periodisch oder kontinuierlich wiederholt. Im Verlauf des Tages verläßt der Nutzer häufig für verschieden lange Zeitspannen seinen Arbeitsplatz. Die Authentisierungsvorrichtung erkennt dies und sperrt sofort für die Zeit der Abwesenheit die Eingabe und/oder Ausgabe der Datenendeinrichtung bei längeren Abwesenheiten wird ein LOGOFF durchgeführt. Zu diesem Zweck wird die Authentisierung des an der Datenendeinrichtung tätigen Nutzers periodisch oder kontinuierlich wiederholt. Verläßt der Nutzer den Wirkungsbereich des Abstandslesers, der maximal einen Meter beträgt, so wird von dem Ansteuerungsprogramm des Abstandslesers beispielsweise die Tastatur gesperrt oder der Bildschirm dunkel getastet. Die Blokkierung erfolgt so lange, bis der Nutzer wieder in den Wirkungsbereich des Abstandslesers zurückkehrt oder durch eine Zeitschaltung des Ansteuerungsprogramms das Abmelden des Nutzers beim System ausgelöst wird.

Die verschiedenen Sperrfunktionen der Datenendeinrichtung können ebenfalls ausgelöst werden, wenn ein nicht autorisierter Nutzer in den Wirkungsbereich des Abstandslesers kommt. Hierzu sind gegebenenfalls weitere Sensoren einzusetzen, die hier nicht beschrieben werden.

Wechseln im Tagesverlauf die Nutzer an einer Datenendeinrichtung, so wird für den jeweils berechtigten Nutzer sofort ein neues LOGON durchgeführt. Jedoch kann der ehemalige Nutzer durch Auslösen einer Sperrfunktion des Abstandslesers diesen Vorgang unterbinden, beispielsweise um einem Mitarbeiter einen Eingabe- oder Ausgabevorgang unmittelbar an der Datenendeinrichtung zu zeigen.

Am Ende des Arbeitstages gibt der Nutzer seinen Identifikationsträger oder seine Kennung an die zentrale Ausgabestelle zurück, wobei seine Kennung abgefragt und dem Datenverarbeitungssystem die Ungültigkeit dieser Kennung mitgeteilt wird.

Der Abstandsleser besteht prinzipiell aus einer Sende- und Empfangsspule sowie einer elektronischen Baugruppe. Typischerweise ist zumindest die Sende- und Empfangsspule sehr nahe bei der Eingabetastatur angebracht. Im Betrieb umgibt sie sich mit einem niederfrequenten magnetischen Wechselfeld, dessen Reichweite typischerweise bei 5—20 cm liegt. Das magnetische Wechselfeld reagiert auf die Anwesenheit des Identifikationsträgers, der am Handgelenk des beispielsweise vor dem Bildschirm sitzenden und die Tastatur berührenden Nutzers angebracht ist.

Die Erfindung wird anhand der Zeichnungsblätter mit den Fig. 1—6 näher beschrieben. Es zeigt

Fig. 1: Die Hauptkomponenten des erfindungsgemäßen Authentisierungssystems

Fig. 2: ein Blockschaltbild des Identifikationsträgers, während er sich im magnetischen Wechselfeld des Schreibgeräts befindet .

Fig. 3: drei verschiedene Bauformen des Identifikationsträgers

Fig. 4: ein Blockschaltbild des Abstandslesers

Fig. 5: eine mögliche Bauform des Abstandslesers

Fig. 6: ein Flußdiagramm des im Abstandsleser benutzten Abfrageprogramms.

In Fig. 1 ist mit DE eine Datenendeinrichtung bezeichnet, die mit einem Datenverarbeitungssystem DV, typischerweise einem zentral aufgestellten Rechner verbunden ist. Als Datenendeinrichtung ist in diesem Ausführungsbeispiel ein Personal-Computer vorgesehen; es kann sich jedoch auch um eine sogenannte Arbeitsstation (work station) oder um ein einfaches Terminal handeln. Im gezeichneten Ausführungsbeispiel steht auf der Zentraleinheit des Personal-Computers ein Bildschirm, während vor der Zentraleinheit in üblicher Weise eine Tastatur TA liegt. Nahe bei der Datenendeinrichtung DE und elektrisch mit ihr verbunden, ist ein Abstandsleser AL angeordnet. Im gezeichneten Ausführungsbeispiel ist ein Abstandsleser AL angeordnet. Im gezeichneten Ausführungsbeispiel ist die Sende- und Empfangsspule 13 des Abstandslesers AL in die Schreibtischunterlage vor der Tastatur TA eingewirkt. Die Sende- und Empfangsspule 13 ist über eine Verbindungsleitung 12 an eine elektronische Baugruppe 2 des Abstandslesers AL angeschlossen, welche als spezifische Prozessor-Karte einschließlich des zugehörigen Sicherheitsprogramms einen Steckplatz des Personal-Computers belegt. Die elektronische Baugruppe 2 kann jedoch auch zusammen mit der Sende- und Empfangsspule 13 in einen Vorlegekeil eingebaut sein, der sich gleichfalls in der Nähe der Tastatur TA befindet. In diesem Fall ist der Abstandsleser AL über eine externe Schnittstelle mit dem Personal-Computer verbunden.

Mit dem Bezugszeichen ID ist ein Identifikationsträger angedeutet, der sich zwangsläufig in der Reichweite des magnetischen Wechselfelds des Abstandslesers AL aufhält, wenn ein Nutzer der Datenendeinrichtung DE ihn am Handgelenk oder in der Nähe des Handgelenks befestigt hat. Mit ZS ist ein zum Abstandsleser AL alternativer Zusatzsensor angedeutet, der es als Option ermöglicht, eine Maussteuerung in die geschützten Eingabefunktionen einzubeziehen.

Der Identifikationsträger ID wird vom Nutzer zum Beispiel in Form einer Uhr oder eines Armbandes getragen. Die Benutzeridentifikation für das LOGON erfolgt im gezeichneten Ausführungsbeispiel, sobald sich der Identifikationsträger ID unmittelbar über der Sende- und Empfangsspule 13 des Abstandslesers AL befindet. Die maximale Abfrageentfernung ist typischerweise kleiner als 20 cm. Die vorbestimmte Entfernung, in welcher die Abfrage der Kennung noch möglich ist, beträgt

in jedem Fall weniger als 1 Meter.

Der Identifikationsträger ID besteht im wesentlichen aus 2 Komponenten. Ein Chip 14 enthält alle zum Betrieb notwendigen elektronischen Bauteile, vorzugsweise in hoch integrierter Form. Die daran angeschlossene Miniaturspule 15 ist wesentlich kleiner als die Sende- und Empfangsspule 13 des Abstandslesers AL, so daß sie zum Beispiel für den Einbau in eine Uhr geeignet ist. Jeder Nutzer, der Zugang zu dem zu schützenden Datenverarbeitungssystem DV erhalten soll, erhält einen Identifikationsträger ID, durch den der Nutzer eindeutig authentisiert werden kann. Diesen Identifikationsträger ID führt der Nutzer möglichst unverlierbar bei sich. Die Miniaturspule 15 tritt im Fall der Abfrage (Fig. 1) mit dem Magnetfeld des Abstandslesers AL in Wechselwirkung. Im Fall der Programmierung (Fig. 2) befindet sich die Miniaturspule 15 im Bereich eines ähnlichen Magnetfelds, das von einem Schreibgerät SG erzeugt wird. In diesem Feld kann der Identifikationsträger ID kontaktlos programmiert werden. Mit dem Schreibgerät SG lassen sich beispielsweise 2^{31} verschiedene Identifikationsträger ID programmieren oder sperren. Änderungen der auf dem Identifikationsträger ID gespeicherten Parameter sind jederzeit möglich. Das Schreibgerät SG kann als eigenständige Datenendeinrichtung des Datenverarbeitungssystems DV konzipiert sein; dann steht es beispielsweise an der Pforte eines Betriebsgebäudes. Das Schreibgerät SG kann aber auch mit dem Abstandsleser AL kombiniert sein; dann ist der Identifikationsträger ID über die Datenschnittstelle zwischen dem Abstandsleser AL und dem Personal-Computer DE programmierbar.

Die Identifikationsträger ID werden mit einem numerischen Code programmiert. Diesen Daten werden Sicherheitsinformationen beigemischt. Die Erzeugung erfolgt nach einer geheimen Formel. Der im Speicher des Identifikationsträgers ID abgelegte Datensatz kann nur einmal hergestellt werden. Dadurch ist die Möglichkeit ausgeschlossen, daß mehrere Identifikationsträger ID mit gleichem Code existieren. Der Nutzer selbst definiert die frei zugänglichen Datenmengen, während das Schreibgerät SG und der Abstandsleser AL für die Datensicherheit des Programmiervorgangs und des Abfragevorgangs sorgen. Ein bestimmter Bereich des Identifikationsträgers ID bleibt dem Anwender verschlossen; dieser Bereich kann nur einmal bei der Herstellung programmiert werden. Diese Sicherheitsmaßnahmen zusammen mit einem ausgeklügelten Polynom für die Datenübertragung erlauben einen betriebssicheren Einsatz.

Der Chip 14 enthält alle zum Betrieb notwendigen Funktionseinheiten. Hierzu gehören ein Speicher für die nutzerspezifische Kennung, eine Sendeschaltung zur Übertragung der gespeicherten Daten, eine Empfangsschaltung zur Änderung von Teilen der gespeicherten Daten und eine Schaltung für die Energiegewinnung zum Betrieb des Chips 14. Der Generator für die Spannungsversorgung des Chips 14 gewinnt die Energie aus dem niederfrequenten magnetischen Wechselfeld. Die integrierte Schaltung 14 speichert im Kennungsspeicher eine mehr als 64 bit (Standardpaßwort) lange, eindeutige Kennung des Nutzers. Diese Kennung liegt nicht flüchtig vor und kann durch Aktivieren des Generators für die Spannungsversorgung ausgelesen werden.

Ein Sendeverstärker liest die Kennungsinformation aus dem Speicher, moduliert sie und übermittelt sie an die Miniaturspule 15. Über dieselbe Schnittstelle läßt sich die gespeicherte Kennung durch Anschließen an das Schreibgerät SG ersetzen. Der Chip 14 und die Miniaturspule 15 sind geschützt in einen Träger eingebaut. Drei mögliche Bauformen des Identifikationsträgers ID sind in Fig. 3 dargestellt. Alle Identifikationsträger ID sind mit einer fest angebrachten Seriennummer ausgestattet.

In Fig. 3.1 sind der Chip 14 und die Miniaturspule 15 wasserdicht in flexibles Material eingegossen. Fig. 3.1 zeigt ungefähr in natürlicher Größe, wie der so entstandene Miniaturträger an einem Armband 16 befestigt werden kann. Ein Kunststoffring 17 umschließt den Identifikationsträger ID und das Armband 16, das beispielsweise ein Uhrarmband ist. Der Miniaturträger 14, 15 kann aber auch mit Hilfe eines nichtmagnetischen Clips an dem Armband 16 befestigt werden.

In Fig. 3.2 ist ein Uhrgehäuse so gestaltet, daß neben dem Uhrwerk 18 zusätzlich der Chip 14 und die Spule 15 in dem Gehäuse Platz finden. Die Spule 15 liegt in diesem Ausführungsbeispiel an der Umfangslinie des Zifferblattes.

Eine weitere Möglichkeit zur Befestigung des Identifikationsträgers ID in Handnähe ist in Fig. 3.3 dargestellt. Der Chip 14 und die Miniaturspule 15 sind in ein eigens dafür angefertigtes, nichtmagnetisches Armband 20 eingebettet. Dieses Armband verfügt über einen Verschluß 19, so daß es außerhalb des Betriebs abgelegt werden kann. Zur weiteren Erhöhung der Sicherheit kann dieser Verschluß mit einem elektronischen Schaltmechanismus kombiniert werden, der die im Chip 14 gespeicherten Informationen löscht, so daß das Armband 20 bei Verlust für den Finder wertlos wird.

Es ist auch denkbar, den Identifikationsträger ID als Fingerring zu realisieren.

In Fig. 4 ist ein Blockschaltbild des Abstandslesers AL dargestellt, der an jede Datenendeinrichtung DE des zu schützenden Systems DV angeschlossen wird. Bei Bedarf kann der Einsatz des Abstandslesers AL auf solche Datenendeinrichtungen DE beschränkt werden, die nicht durch sonstige Maßnahmen hinreichend geschützt sind oder bei denen ein häufiger Wechsel des Nutzers vorkommt.

Der Abstandsleser AL setzt sich im wesentlichen aus der elektronischen Baugruppe 2 und der Sende- und Empfangsspule 13 zusammen. Die Sende- und Empfangsspule 13, die aus Kupferdraht besteht, ist über eine zweiadrige Verbindungsleitung 12 mit der elektronischen Baugruppe 2 verbunden. Die elektronische Baugruppe 2 ihrerseits setzt sich in der Hauptsache aus einer Sende- und Empfangsschaltung 8 und einem Mikroprozessor 3 zusammen. Die Sende- und Empfangsschaltung 8 enthält einen Generator 9 mit Leistungsverstärker 10, der das niederfrequente magnetische Wechselfeld in der Sende- und Empfangsspule 13 erzeugt. Das vom Identifikationsträger ID in die Sende- und Empfangsspule 13 eingekoppelte Signal wird über eine Empfangsschaltung 11 so weit aufbereitet, daß es vom Mikroprozessor 3 ausgewertet werden kann.

Der Mikroprozessor 3 besteht im wesentlichen aus einer CPU 5, einem EEPROM 6 zur Speicherung des Abfrageprogramms, einem RAM 7 als Arbeitsspeicher sowie aus einem Schnittstellenbaustein 4. Der Schnittstellenbaustein 4 betreibt, zusammen mit dem Abfrageprogramm, die Schnittstelle 1. Über diese Schnittstelle 1 wird der Abstandsleser AL an den Personal-Computer oder an eine sonstige Datenendeinrichtung DE angekoppelt. Bei einer bereits realisierten Version ist die Schnittstelle 1 als V.24-Schnittstelle zu einem Personal-Computer realisiert. Bei der in Fig. 1 dargestellten Ver-

sion, bei der die elektronische Baugruppe 2 des Abstandslesers AL als Steckkarte in die Datenendeinrichtung DE eingesetzt wird, wird die Schnittstelle 1 als interne Bus-Schnittstelle ausgeführt.

Im Betrieb wird über die Leistungskette 9, 10, 12, 13 ein Wechselmagnetfeld begrenzter Reichweite erzeugt, das in der Miniaturspule 15 des Identifikationsträgers ID eine Wechselspannung erzeugt. Diese Wechselspannung wird im Chip 14 in die erforderliche Betriebsspannung umgesetzt. Der Identifikationsträger ID sendet daraufhin die in ihm gespeicherte Nutzerkennung in binärer Form aus. Die Daten werden vom Empfangszweig 13, 12, 11 des Abstandslesers AL empfangen und im Mikroprozessor 3 aufbereitet und ausgewertet. Der Mikroprozessor 3 steuert über die Schnittstelle 1 die Datenendeinrichtung DE an und löst dort frei programmierbare Folgeaktionen aus, die im Zusammenhang mit dem Funktionsflußdiagramm gemäß Fig. 6 besprochen werden.

Fig. 5 zeigt eine zu Fig. 1 alternative Ausführungsform des Abstandslesers AL. Es handelt sich um ein keilförmiges Gehäuse 23, in dem sowohl die Sende- und Empfangsspule 13 als auch die elektronische Baugruppe 2 untergebracht sind. Das Gehäuse 23 besteht aus mitteldichter Faserplatte (MDF) und wird als Vorlegekeil vor die Tastatur TA eines tragbaren Personal-Computers gelegt. Eine grüne Leuchtdiode 21 auf der Oberseite des Gehäuses 23 zeigt die Anwesenheit eines Identifikationsträgers ID im Wirkungsbereich der Sende- und Empfangsspule 13 an. Der Anschluß an den Personal-Computer erfolgt mit Hilfe eines aus dem Gehäuse 23 herausgeführten Verbindungskabels 22. Das Verbindungskabel 22 wird mit einer der seriellen Schnittstellen des Personal-Computers verbunden.

Das Flußdiagramm in Fig. 6 zeigt die wichtigsten Funktionen des im Abstandsleser AL enthaltenen Abfrageprogramms. Im Zustand a "kein Nutzer" ist keine Person mit dem Datenverarbeitungssystem DV in Verbindung getreten. Die Dateneinrichtung DE ist für alle Eingaben gesperrt und keine ihrer Anwendungen ist aktiv. In der Funktion b überprüft die CPU 5 fortlaufend das Signal des Empfängers 11 daraufhin, ob ein Identifikationsträger ID in den Wirkungsbereich der Sende- und Empfangsspule 13 eintritt. Falls ein Identifikationsträger ID detektiert wird, wird die Funktion c aktiv. Mit Hilfe einer Datenbasis, die entweder im EEPROM 6 oder auf den Speichermedien des Personal-Computers DE oder im zentralen Speicher des Datenverarbeitungssystems DV abgelegt ist, wird geprüft, ob die Kennung dieses Nutzers für diese Datenendeinrichtung DE zugelassen ist. Falls nicht, bleibt das Gerät DE gesperrt und es wird gewartet, bis eine neue Kennung detektiert wird.

Falls die Kennung zugelassen ist, wird im Zustand d die Datenendeinrichtung zur Nutzung freigegeben. Die Anwesenheit des Identifikationsträgers ID im Wirkungsbereich der Sende- und Empfangsspule 13 wird durch die Funktion e fortlaufend überwacht. Sobald der Nutzer den Wirkungsbereich verläßt, wird die Datenendeinrichtung DE in näher zu bestimmender Weise gesperrt und auf die Detektion einer weiteren Nutzerkennung gewartet. Der Wirkungsbereich eines Gehäuses 23 oder einer entsprechenden Schreibtischunterlage oder einer sonstigen Bauform der Sende- und Empfangsspule 13 beträgt typischerweise weniger als 20 cm, überschreitet aber aus Sicherheitsgründen in keinem Fall die Entfernung von einem Meter.

Unter dem Blockieren der Datenendeinrichtung welches sofort ausgelöst wird, ist insbesondere ein Sperren der Tastatur und/oder ein Dunkeltasten des Bildschirms zu verstehen. Diese Sperren werden wieder aufgehoben, wenn der Nutzer in den Wirkungsbereich zurückkehrt. Nach Ablauf einer bestimmten Zeit (z. B. drei Minuten) kann das Abfrageprogramm den Nutzer beim Datenverarbeitungssystem DV abmelden (LOGOFF). Bei besonders sicherheitsempfindlichen Datenendeinrichtungen kann auch registriert werden, wenn sich der Nutzer kurzzeitig von der Datenendeinrichtung DE entfernt und diese gesperrt wird. Die Funktion "Sperren der Tastatur/Dunkeltasten des Bildschirms" kann auch ausgelöst werden, wenn ein nicht autorisierter Nutzer in den Wirkungsbereich des Abstandslesers AL kommt. Hierzu sind ggf. weitere Sensoren einzusetzen.

Neben dem automatischen Sperren der Datenendeinrichtungen gibt es für den Nutzer natürlich die Möglichkeit, eine Sitzung explizit zu beenden. Die Funktion f entscheidet darüber, ob alle aktiven Anwendungen beendet werden oder ob die automatischen Sperrfunktionen auslösbar bleiben. Weitere Sperrfunktionen oder Folgeaktionen sind programmierbar, beispielsweise über die Schnittstelle 1 von der Datenendeinrichtung her.

Patentansprüche

1. System zur Authentisierung des Nutzers einer Datenendeinrichtung eines Datenverarbeitungssystems,
bei dem der Nutzer einen Identifikationsträger, der innerhalb einer vorbestimmten Entfernung berührungslos abgefragt werden kann, schwer verlierbar mit sich trägt,
und bei dem ein Abstandsleser, der nahe bei der Datenendeinrichtung angebracht und über ein Verbindungskabel mit der Datenendeinrichtung verbunden ist, eine persönliche Nutzerkennung auf dem Identifikationsträger sich innerhalb der vorbestimmten Entfernung befindet,
dadurch gekennzeichnet, daß
ein Schreibgerät (SG) zu vorgegebenen Zeitpunkten (z. Bsp. täglich) eine neue persönliche Nutzerkennung auf dem Identifikationsträger (ID) einprogrammiert und gleichartig an das Datenverarbeitungssystem (DV) übermittelt,
der schwer verlierbare Identifikationsträger (ID) in der Nähe des Handgelenks des Nutzers angebracht ist,
die vorbestimmte Entfernung zwischen Identifikationsträger (ID) und Abstandsleser (AL) und damit auch die Entfernung zwischen Identifikationsträger (ID) und Datenendeinrichtung (DE) weniger als 1 Meter beträgt
und sowohl die Abfrage als auch die Programmierung der persönlichen Nutzerkennung durch ein magnetisches Wechselfeld vermittelt wird.

2. Authentisierungssystem nach Anspruch 1, dadurch gekennzeichnet, daß die genutzte Datenendeinrichtung ein Personal-Computer ist.

3. Authentisierungssystem nach Anspruch 1, dadurch gekennzeichnet, daß die genutzte Datenendeinrichtung eine Workstation ist.

4. Authentisierungssystem nach Anspruch 1, dadurch gekennzeichnet, daß die genutzte Datenendeinrichtung ein Terminal ist.

5. Authentisierungssystem nach Anspruch 1 bis 4, dadurch gekennzeichnet, daß das Schreibgerät

(SG) die erzeugte Nutzerkennung an die zentrale Datenbasis des Datenverarbeitungssystems (DV) übermittelt.

6. Authentisierungssystem nach Anspruch 1 bis 4, dadurch gekennzeichnet, daß das Schreibgerät (SG) mit dem Abstandsleser (AL) kombiniert ist und die erzeugte Nutzerkennung an die Datenbasis im Abstandsleser (AL) übermittelt.

8. Authentisierungssystem nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die vorbestimmte Entfernung zwischen dem Identifikationsträger (ID) einerseits und dem Abstandsleser (AL) bzw. der Datenendeinrichtung (DE) andererseits weniger als 20 cm beträgt.

9. Authentisierungssystem nach Anspruch 1 bis 8, dadurch gekennzeichnet, daß die Datenendeinrichtung (DE) sofort gesperrt wird, wenn der Identifikationsträger (ID) die vorbestimmte Wirkungsentfernung verläßt.

10. Authentisierungssystem nach Anspruch 9, dadurch gekennzeichnet, daß die Eingabetastatur (TA) blockiert wird.

11. Authentisierungssystem nach Anspruch 9, dadurch gekennzeichnet, daß ein Bildschirm der Datenendeinrichtung (DE) dunkelgetastet oder ein Drucker der Datenendeinrichtung (DE) gesperrt wird.

12. Authentisierungssystem nach Anspruch 9, dadurch gekennzeichnet, daß die Datenendeinrichtung (DE) den Nutzer nach Ablauf einer bestimmten Zeitspanne beim Datenverarbeitungssystem (DV) abmeldet.

13. System zur Authentisierung, mit welchem der Nutzer eines Datenverarbeitungssystems, der sich in der Nähe einer Datenendeinrichtung befindet, berührungslos authentisiert wird, gekennzeichnet durch
einen Identifikationsträger (ID), der aus einem Chip (14) und einer Miniaturspule (15) besteht,
einen Abstandsleser (AL), bei dem eine elektronische Baugruppe (2) über eine Verbindungsleitung (12) an eine Sende- und Empfangsspule angeschlossen ist,
und ein Schreibgerät (SG) zum Programmieren des Identifikationsträgers (ID), welches zentral oder über die Datenendeinrichtung (DE) an das Datenverarbeitungssystem (DV) angeschlossen ist.

14. System nach Anspruch 13, dadurch gekennzeichnet, daß der Identifikationsträger (ID) an einem Armband (16) befestigt ist.

15. System nach Anspruch 14, dadurch gekennzeichnet, daß die Befestigung durch einen Kunststoffring (17) geschieht.

16. System nach Anspruch 14, dadurch gekennzeichnet, daß die Befestigung durch einen nichtmagnetischen Clip geschieht.

17. System nach Anspruch 13, dadurch gekennzeichnet, daß der Identifikationsträger (ID) in ein Armband (20) eingebaut ist.

18. System nach Anspruch 17, dadurch gekennzeichnet, daß das Armband (20) einen Verschluß (19) aufweist, bei dessen Öffnen die Kennung im Identifikationsträger (ID) gelöscht wird.

19. System nach Anspruch 13, dadurch gekennzeichnet, daß der Identifikationsträger (ID) neben einem Uhrwerk (18) in einem Uhrgehäuse eingebaut ist.

20. System nach Anspruch 13, dadurch gekennzeichnet, daß der Identifikationsträger (ID) in einem Fingerring eingebaut ist.

21. System nach Anspruch 13 bis 20, dadurch gekennzeichnet, daß der Abstandsleser (AL) in einem Gehäuse (23) untergebracht ist, das eine elektronische Baugruppe (2) und eine Sende- und Empfangsspule (13) enthält und als Vorlegekeil ausgebildet ist.

22. System nach Anspruch 21, dadurch gekennzeichnet, daß das Gehäuse (23) eine Leuchtdiode (21) trägt, welche die vollzogene Authentisierung des Nutzers anzeigt.

23. System nach Anspruch 13 bis 20, dadurch gekennzeichnet, daß die Sende- und Empfangsspule (13) des Abstandslesers (AL) in eine Schreibtischunterlage eingewirkt ist, und daß die elektronische Baugruppe (2) des Abstandslesers (AL) auf einer Steckkarte angeordnet ist, welche in die Datenendeinrichtung (DE) einsteckbar ist.

24. System nach Anspruch 13 bis 23, dadurch gekennzeichnet, daß ein Zusatzsensor (ZS) vorgesehen ist, der für die Annäherung des Identifikationsträgers (ID) an eine weitere Eingabevorrichtung, insbesondere eine sog. Maus, empfindlich ist.

25. System nach einem der Ansprüche 13 bis 24, dadurch gekennzeichnet, daß weitere Sensoren vorgesehen sind, welche die Annäherung von nichtberechtigten Personen registrieren.

26. System nach Anspruch 13 bis 25, dadurch gekennzeichnet, daß die elektronische Baugruppe (2) des Abstandslesers (AL) über eine serielle Schnittstelle an die Datenendeinrichtung (DE) angeschlossen ist.

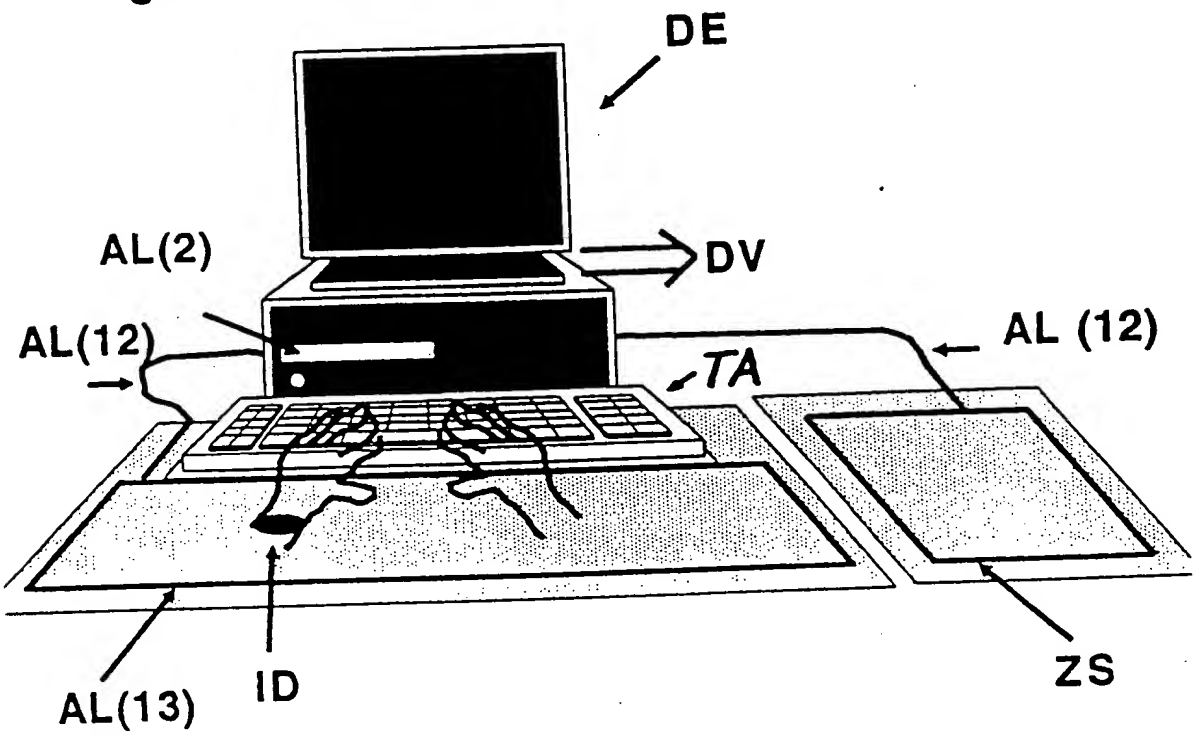
27. System nach Anspruch 13 bis 25, dadurch gekennzeichnet, daß die elektronische Baugruppe (2) des Abstandslesers (AL) über eine interne Schnittstelle an den Datenbus der Datenendeinrichtung (DE) angeschlossen ist.

Hierzu 5 Seite(n) Zeichnungen

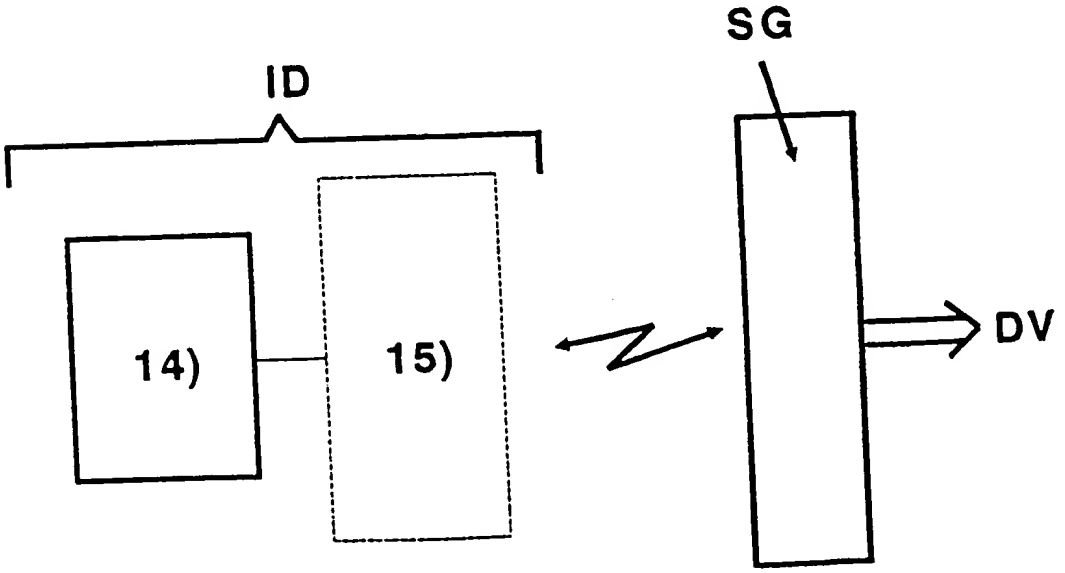
— Leerseite —

Nummer DE 40 15 482 C1
Int. Cl.[5]. G 06 F 12/14
Veröffentlichungstag: 25. Juli 1991

Figur 1: Hauptkomponenten



Figur 2: Blockschaltbild des ID-Trägers

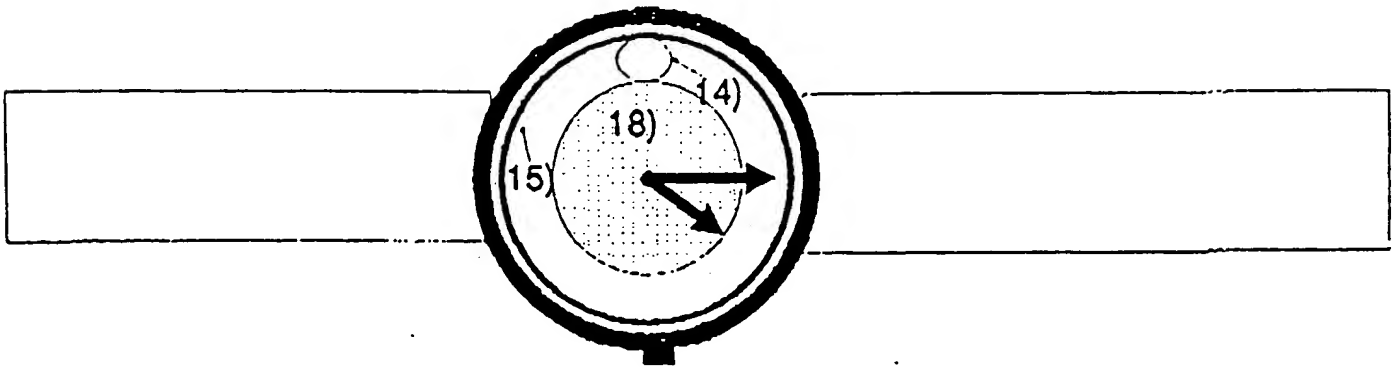


Nummer DE 40 15 482 C1
Int. Cl.[5]: G 06 F 12/14
Veröffentlichungstag: 25. Juli 1991

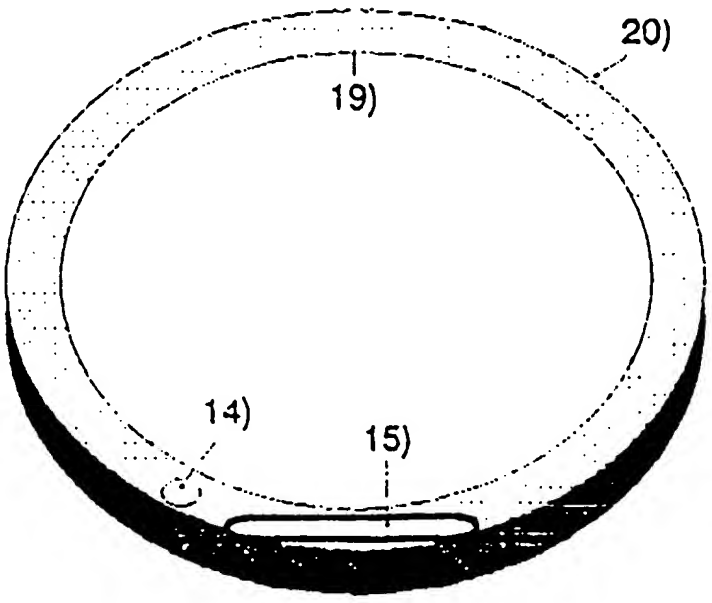
Figur 3: Bauformen des ID-Trägers

Figur 3.1: Befestigung am Armband

Figur 3.2: in Uhr integriert

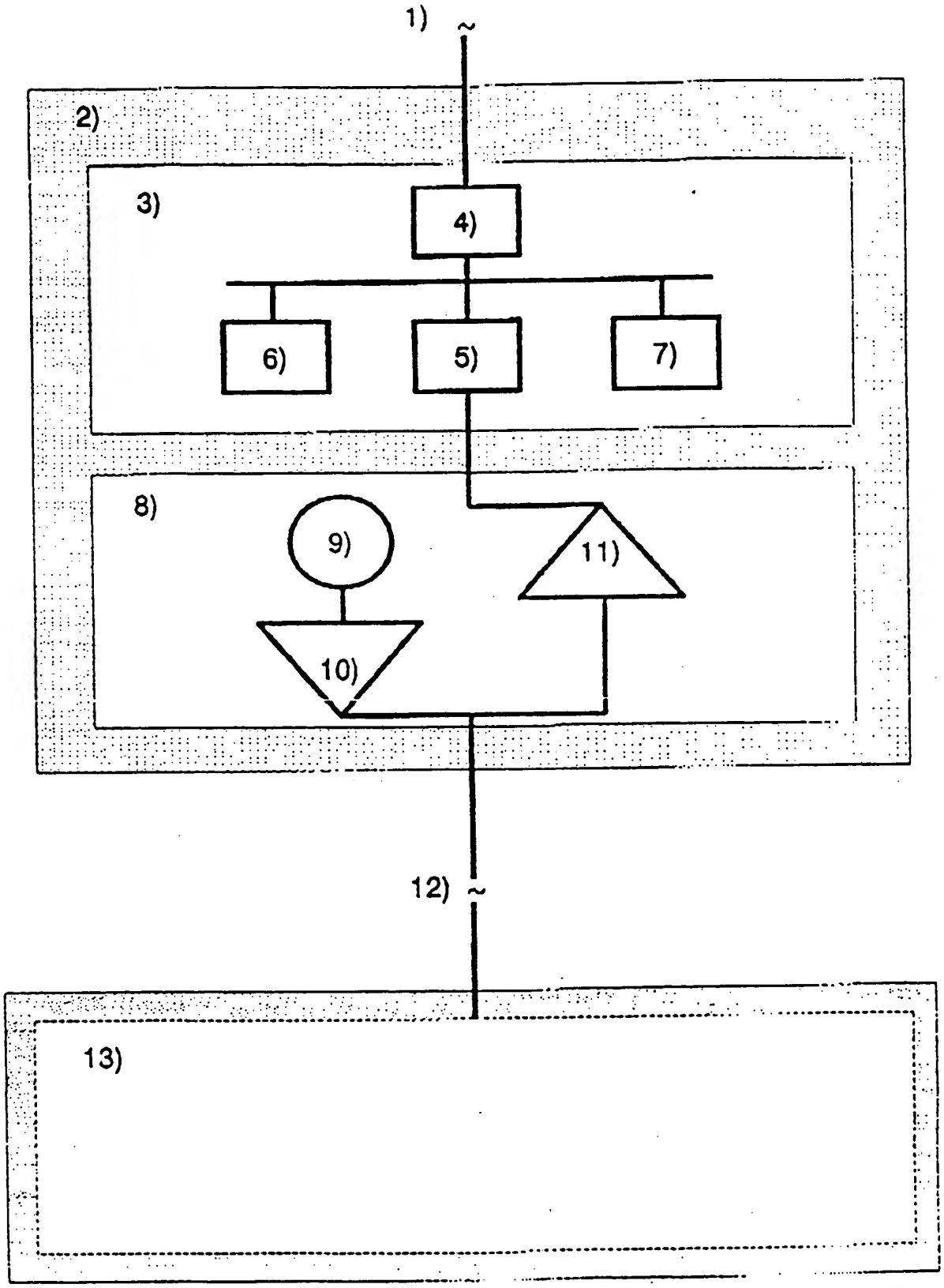


Figur 3.3: in Armband integriert



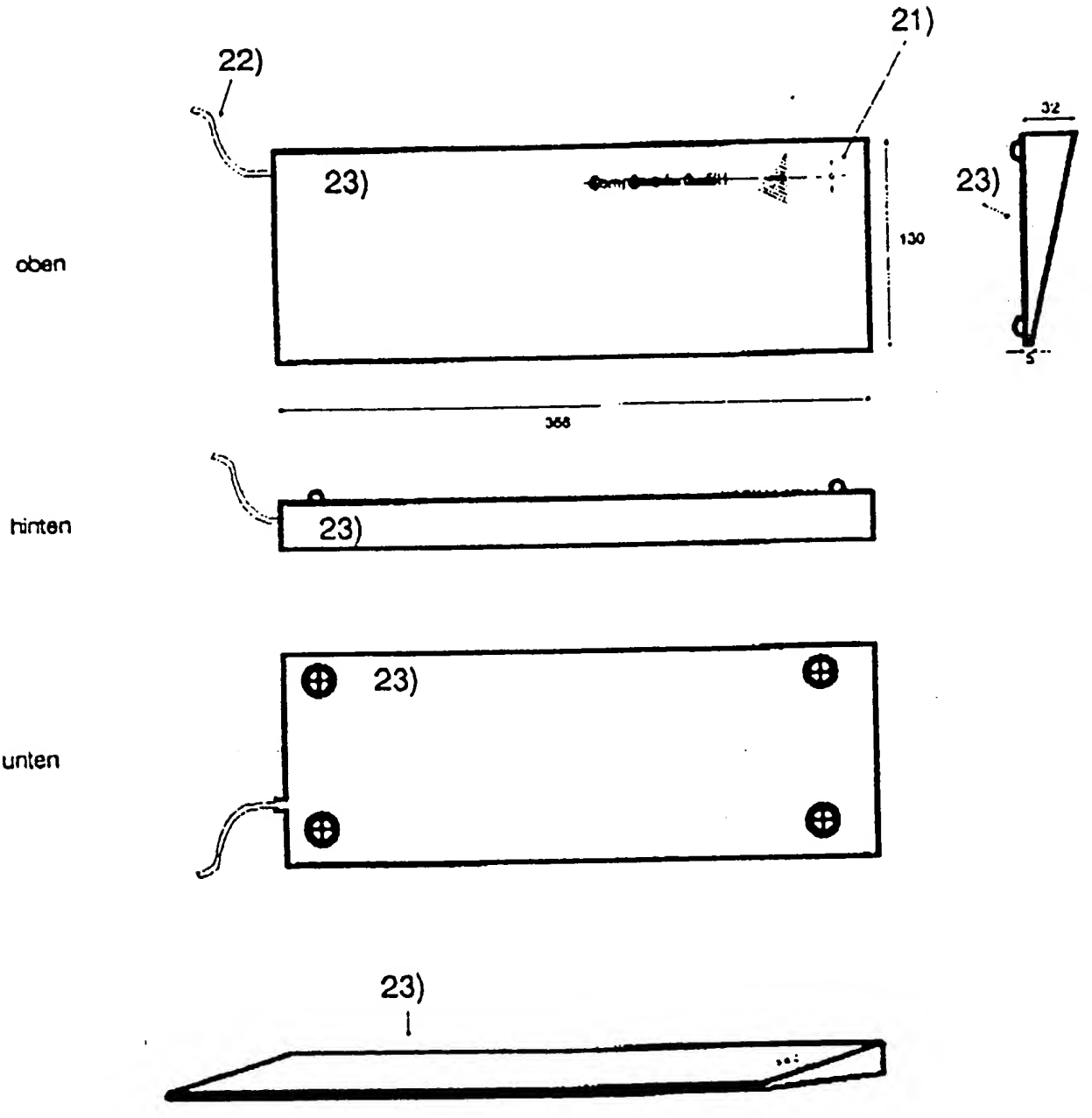
Nummer: DE 40 15 482 C1
Int. Cl.[5]: G 06 F 12/14
Veröffentlichungstag: 25. Juli 1991

Figur 4: Blockschaltbild des Abstandslesers



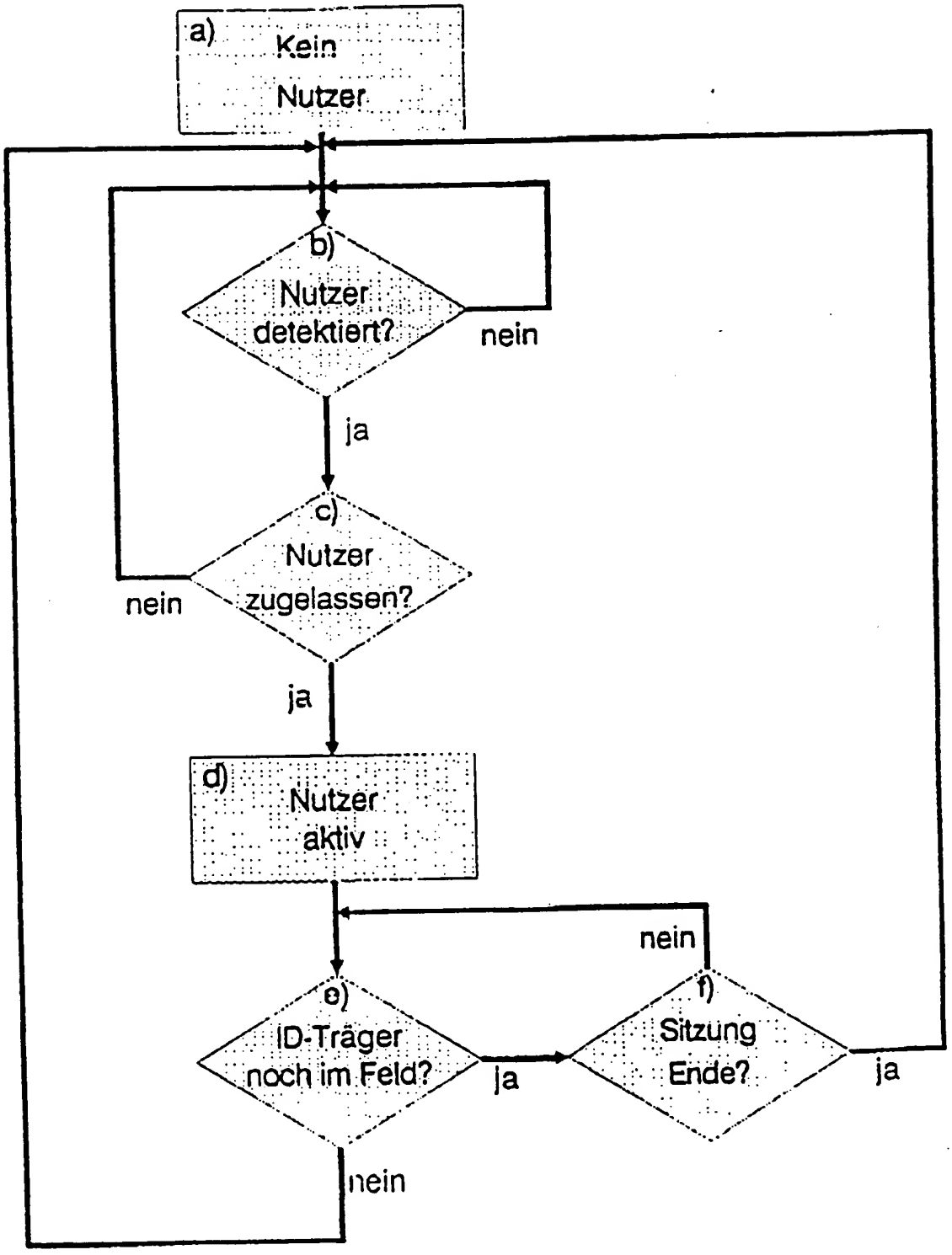
Nummer: DE 40 15 482 C1
Int. Cl.[5]: G 06 F 12/14
Veröffentlichungstag: 25. Juli 1991

Figur 5: Gehäuse für Abstandsleser



Nummer DE 40 15 482 C1
Int. Cl.[5]: G 06 F 12/14
Veröffentlichungstag: 25. Juli 1991

Figur 6: Funktionsflußdiagramm



(12) **Patent Text**

(11) **DE 40 15 482 C1**

(19) **Republic of Germany**
German Patent Office

(51) **Int.Cl[6]:**
G 06 F 12/14
G 07 C 9/00

(21) **File No.:** **P 40 15 482.3-53**
(22) **Date of Application** **May 14, 1990**
(43) **Date of Declaration** ——
(45) **Patent issue date** **July 25, 1991**

(73) Owner of patent: Competence Center Informatik, GmbH
4470 Meppen, Germany

(74) Patent Attorney(s)
Pagenberg, J. Dr. Jur.; Frohwitter, B., Dipl.-Ing., Atty.,
Geißler, B. Dipl.-Phys.Dr. Jur., Pat. & Atty,,
Bardehle, H. Dipl. Ing.; Dost, W., Dipl. Chem, Dr. Rer nat
Altenburg, U., Dipl.-Phys., Patent Anwalt, Munich

Inventor
Holzapfel, Stephan, 4470 Meppen, DE
Book, Norbert, 4530 Ibbenbüren, DE
Kraaibeek, Peter, 4450 Lingen, DE

For judgement as to patentability the following were considered:
US-Z IBM Technical Disclosure Bulletin, Vol. 31
No. 9, February 1989, Page 223
DE-Z Funkshau (Radio Show) 13/1986, Pages 24 - 28
House organ Unine, Unisses a revolutionary 100%
watertight security system for your personal computer.

(54) Title: A system for touch-free authenticating of the user of a data terminal apparatus of a data processing procedure

Proposed is a system for a touch-free authenticating of the user of a data terminal apparatus of a data processing procedure. The user wears an identification carrier, designed to be difficult to lose, which can be electronically interrogated within a distance of less than 1 m. A distance detector, which is installed in proximity to the data terminal apparatus and is connected thereto by a cable, continually interrogates the personal user recognition from the identification carrier. When the pre-specified separation distance is overstepped for a given time, then the data terminal apparatus is partially or completely blocked. A registering device programs the said identification carrier at specified intervals , at which the user is repeatedly identified. The registering device transmits the produced user recognition to the data processing system. The identification carrier is placed in a magnetic alternating field not only for the interrogation, but also for the programming of the personal user recognition device.

Patent DE 40 15 482 C1

"A system for touch-free authenticating of a user of a data terminal of a data processing system"

Description

The invention concerns a system for touch-free authentication of a user of a data terminal apparatus of a data processing system, as this is presented in the generic concept of Claim 1 of the present patent. A system of this type is made known by a house organ of the firm UNINA, in which a security system UNISES is described. The invention further concerns a system for authentication in accord with the generic concept of Claim 13 of this present patent.

In order to protect endangered or otherwise protection worthy data processing systems from unauthorized entry, conventionally the so-called LOGON-process has been employed. By this process, user recognitions and passwords were input to a data terminal apparatus of the data processing system, to which the authorized user and the system were known. That system identified the user with the aid of his password and assured him of access rights to his assigned data terminal apparatus.

This process exhibits points of weakness, by which the password can easily be circumvented, namely:

- Simple passwords can be easily detected, the protection of the system from unauthorized users is not assured,
- Efficient, and thereby long passwords are easily forgotten by the user. Therefore, these are frequently placed in written form and can on this account also be discovered,
- Users, who have forgotten their identification feature "Password" are not available to the system in critical situations,

- The procedure of the LOGON is time consuming for the user and diverts him from the reality of the intended purpose of the data system and

- Passwords can be inferred upon input by keyboard by observation of finger movements.

The above outlined, inadequate measures cause the authorized usage of the data processing system to be uncomfortable. The result of this is the limited or inadequate employment of the safety measures which have been available.

The present safety deficiencies have led to considerations, as to how data security for the user can be fundamentally improved. The method mentioned in the above introduction, "UNISES" dispenses with the manual input of passwords and authenticates the user of a personal computer automatically. The apparatus is comprised of an integrated switching circuit, which is built into the said Personal computer and is provided with serviceable key functions, as well as being comprised also of a small high frequency sender, which is carried in the pocket of the authorized user and emits a personal recognition signal. The high frequency sender has a field extent of five meters and the radio connection (for that is what it is) is further protected by key-algorithms. When the Personal computer identifies an authorized user, the recognition is transferred out of the identification carrier into the key-chip and thereupon, the standard functions of the Personal computer as well as the protected data areas stand available to the approved user. The authentication is

[German Column No. 2]

continually repeated. When the user vacates his work place, then the Personal computer carries on the normal data processing, however, it blocks every entry into the input function, i.e. the functioning of the keyboard.

This authorization procedure already fulfills some of the conditions which are to be applied to improved data protection. Especially, a difference is made between authorized and non-authorized personnel, while the user is spared the complicated and time robbing recognition input procedures.

When the authorized user leaves the computer site, then the computer automatically drops into its safety-sensitive operative mode, blocking access as above described. Disadvantageously, to the known process, is the active, i.e. self powered sender which is battery driven and thus not maintenance free. This sender is also thereby made comparatively large in size. A further deficiency, is that the unknown process is not open for further authentication steps. These steps increase in importance in proportion to how much larger becomes the data processing system to which data terminal apparatus is connected. From the IBM Technical Disclosure Bulletin of February, 1989, page 223 and from the Funkshau bulletin 13/1986, pages 24 to 29, small, passive (no battery) identification carriers are disclosed.

Therefore, the invention takes upon itself the purpose of further improving protection against loss or hostile observation of personal use recognition, by means of a touch-free, authenticating system of the above mentioned characteristics. This purpose will be achieved by the recognition features of Claim 1 in connection with inherent features of data protection procedures. A subordinate embodiment of the concept of the invention is presented in Claim 13 of the present patent.

The invented identification carrier is passive, maintenance free and not larger than 3 x 15 x 20 mm. In the case of the system in accord with the invention, the user recognition can be changed frequently, possibly daily. In this case the user recognition is emitted from a station, which unmistakably identifies the user daily on the grounds of other characteristics. In this matter the new user recognition is produced by a registration apparatus at a plant wide dissemination station, thus automatically transmitting the personal authorization through the said station into the invented system. The registration station can be combined with a distance detector, which reads the recognition off of the identification carrier and transmits these data to the data terminal apparatus.

For the daily authentication of the user by acceptance of the recognition, biometric identification procedures may be brought to bear. If these prove too costly for each data terminal apparatus, then the biometric identification can be an automatic evaluation of the signature.

In a typical application example, a data processing user enters the company building of his firm and identifies himself at the entry by his signature. Instead of an automatic evaluation of the signature, there is also a personal identification to be considered. He thereupon receives an identification carrier, or, in case he already has such a device, he receives a new recognition input for the use of the firm's data processing system. The recognition is programmed in by a registration device and together with the identity of the user, is transmitted to the data processing system. The system, where necessary, provides the daily recognition of this user to appropriate other systems he might use.

[German Column No.3]

The identification carrier is bound on the wrist of the user and is hard to lose. For instance, the identification carrier can be affixed to a watch, or an arm band or even a ring. After the acceptance of the identification carrier or the new recognition, the user proceeds to his work station. The data terminal apparatus recognizes the user by the signal emitted by the identification carrier. In this procedure, a distance detector is installed in the data terminal apparatus, which unmistakably identifies each user proximal to the data terminal apparatus. The distance detector is controlled by a special program, which immediately and automatically releases the LOGON process through the data terminal for the identified user. The user then, without delay, can start with his work in the data processing system. Where a fully automatic recognition system is not advantageous, the LOGON process can be called up by the user. The running of the LOGON process is displayed on the data terminal equipment.

In the communication between the data terminal and the computer, during the LOGON procedure, cryptographic programs can be brought into play, which make difficult a discovery of the use-recognition by tapping wires.

The authentication of the user working on the data terminal apparatus is periodically or continually reviewed. In the course of the day, the user frequently leaves his workplace for time spans of various lengths. The authentication apparatus detects this and, for the time of the absence of input and/or output to the data terminal apparatus, activates a LOGOFF procedure.

For this purpose, the authorization of the active user on the data terminal apparatus is periodically or continually reviewed. If the user leaves the active zone of the distance detector area, which is one meter maximal, then the control program of the distance detector area will block the keyboard and/or render the monitor screen dark. This blockage remains so, until the user returns to the area of the distance detector, or, by means of a time switch, the control program will release the quitting signal of the user and shut down the system.

The various blockage functions of the data terminal apparatus can be released, in like manner, when a non-authorized person comes into the active field of the distance detector. In this case, where required, additional sensors can be located, which will not be described here.

If, in course of the day, there is a change of user on a data terminal apparatus, then, if said new user is authorized, then immediately another LOGON is carried through. However, the former user, by the release of a blockage function of the distance detector, can accommodate this procedure, for instance in order to show a co-worker an input or an output process directly on the data terminal apparatus.

At the end of the workday, the user returns his identification carrier or his recognition device back to the central issuance station, whereby his recognition is challenged and the data processing system is informed of the invalidity of this recognition signal.

The distance detector is comprised principally of a sending and receiving coil as

[German Column No.4]

an electronic subassembly. Typically, at least the sending and receiving coil is installed very near to the input keyboard. In operation, this is surrounded by a low frequency, magnetic alternating field, the active extent of which is typically 5 to 20 cm. The magnetic alternating field reacts to the presence of the identification carrier, which is placed on the wrist of the user sitting, for example, before the screen and operating the keyboard.

The invention will be described in greater detail with the help of reference to the

drawings, especially Figs. 1 to 6. There is shown in:

Fig. 1 the main components of the authentication apparatus in accord with the invention,

Fig. 2 a block circuit diagram of the identification carrier, while it is in the magnetic alternating field of the registration apparatus,

Fig. 3 three identification carriers, each constructed differently,

Fig. 4 a block diagram of the distance detector,

Fig. 5 a possible embodiment of the distance detector and

Fig. 6 a logic diagram of the employed interrogating program in the distance detector.

In Fig. 1, the data terminal apparatus is designated as DE, which is connected, in a typical manner, with a data processing system DV, this being normally a centrally placed computer. A personal computer is foreseen, in this embodiment of the present patent, as a data terminal apparatus. This may just as well be a so-called workstation or a simple terminal. In the depicted embodiment on the central unit of the Personal computer is a monitor with screen, while, in front of the said central unit is, as usual, a keyboard TA. In proximity to the data terminal apparatus DE and electrically connected therewith is located a distance detector AL. A distance detector AL is shown in the illustrated example. In the drawn embodiment is shown the sending and receiving coil 13 of the distance detector AL, worked into the desk surface in front of the keyboard TA. The sending and receiving coil is connected by an electrical cable 12 to an electronic subassembly 2 of the distance detector AL, which possesses a slot in a Personal computer, as a specific processor card, including the associated safety program. The electronic subassembly can also be concealed in a front wedge, along with the sending and receiving coil 13, which likewise finds itself in proximity to the keyboard TA. In this case, then the distance detector AL is connected by means of an external interface with the personal computer.

ID designates an identification carrier, which necessarily maintains a position in the active zone of the magnetic alternating field of the distance detector AL, when a user of the data terminal apparatus DE has it on his wrist or in proximity of the wrist. ZS denotes an alternative sensor to the distance detector AL, which offers the option of bringing a mouse into the protected input functions.

The identification carrier ID is found directly over the sending and receiving coil 13 of the distance detector AL. The maximum interrogation distance is typically less than 20 cm. The prespecified distance, in which interrogation regarding identity is still possible, is in any case, less than 1 meter.

[German Column No.5]

The identification carrier ID is comprised essentially of 2 components. A chip 14 contains all necessary electronic subassemblies necessary for operation, advantageously in a highly integrated form, The miniature coil 15 is essentially smaller than the sending-receiving coil 13 in the distance detector AL, so that it is, for example, suitable for integrating inside of a watch. Each user, who should have access to the protected data processing system DV, receives an identification carrier ID, by means of which the authenticity of the user can be reliably determined. This identification carrier the user is to carry with him in a manner which prevents loss as far as possible. The miniature coil 15, in the case of interrogation, (Figs 1, 2) enters into the alternating magnetic field of the distance detector AL. In the case of programming (Fig. 2), the miniature coil 15 finds itself in a similar magnetic field, which has been produced by the registration apparatus SG. In this field, the identification carrier ID can be touch-free programmed. With the registration apparatus SG, for instance 2^{31} different identification carriers ID can program or block. Alterations in the stored parameters on the identification carrier ID can be effected at any time. The registration apparatus SG can be conceived also as a self contained data terminal apparatus of the data processing system DV. In this case, it is positioned at the gate of a company building.

The registration apparatus SG can, however, be combined with the distance detector AL, in which case the identification carrier ID is programmable through the data interface between the distance detector AL and the personal computer DE.

The identification carrier ID is programmed with a numerical code. To these data was added the security information. The output is determined by a secret formula. The data record which is placed in the memory of the identification carrier ID can only be generated once. Thereby, the possibility is excluded, that several identification carrier ID could exist with the same code. The user himself defines the freely accessible quantities of data while the registration apparatus SG and the distance detector AL attend to the data security of the program procedure and the interrogation. A particular range of the identification carrier ID remains closed to the user. This range, again, can only be programmed for the one time it is called up. These security measures, together with an ingenious polynomial for the data transmission permit a operationally safe installation.

The chip 14 contains all functional components necessary for operation. To this belong memory storage for the user-specific recognition, a sending circuit for the transmission of the stored data, a receiving circuit for the alteration of parts of the stored data and a circuit for the energy yield for the operation of the chip 14. The generator for the voltage supply to chip 14 obtains the energy from the low frequency, alternating magnetic field. The integrated circuit 14 stores in the identification storage the identification memory defining the user, this being a more than 64 bit long (standard password), unmistakable recognition of the user. This recognition is not volatile and can be read-out by the activation of the generator for the voltage supply.

A sending amplifier reads the recognition information from the storage, modulates it, and transmits it to the miniature coil 15. Over the same interface connection, the stored recognition is transmitted to the registration apparatus SG. The chip 14 and the miniature

[German Column No. 6]

coil 15 are protectively installed within a carrier. Three possible modes of construction of the identification carrier ID are presented in Fig. 3. All identification carriers ID are marked with a firmly applied serial number.

In Fig. 3.1 the chip 14 and the miniature coil 15 have been cast into water tight, flexible material. Fig. 3.1 shows, approximately in natural size, how the miniature carrier, so constructed, can be affixed onto an armband 16. A plastic ring 17 encapsulates the identification carrier and the armband 16, which armband 16, for instance can be a wristwatch band. The miniature carrier 14, 13 can, however, be affixed to the arm band 16 with the help of non magnetic clips.

In Fig. 3.2 a watch housing is so adapted, that beside the clockwork 18, additionally the chip 14 and the coil 15 can find a place in the housing. The coil 15 lies in this embodiment on the outside circumferential line of the dial.

A further possibility for the fastening of the identification carrier ID in proximity to the hand is found pictured in Fig. 3.3. The chip 14 and the miniature coil 15 are embedded in a non-magnetic armband 20, which said armband is fashioned for this service. This armband possesses a closure 19, so that it can be taken off outside of the place of business.

For a further increase of the security, this closure can be combined with an electronic circuit, in which the stored information in chip 14 is erased, so that the arm band 20, upon loss, is worthless for the finder.

Consideration can also be given to constructing the identification carrier ID as a finger ring.

In Fig. 4 is presented a block diagram of the distance detector AL, which is connected to each data terminal apparatus DE of the system to be protected. Upon need, the installation of the distance detector AL can be limited to such data terminal apparatuses DE as are not sufficiently protected by other measures or by those in which a frequent change of operators occurs.

The distance detector AL is comprised of a combination of the electronic subassembly 2 and the send and receive coil 13 as pictured in Fig. 4. The send and receive coil, which is made of copper wire, is attached by a two line connector 12 with the electronic subassembly 2. The electronic subassembly 2 is mainly a combination of a send/receive circuit 8 and a microprocessor 3.

The send and receive circuit 8 contains a generator 9 with a power amplifier 10, which produces the low frequency, alternating magnetic field in the send and receiving coil 13. The signal launched from the identification carrier ID in the send and receive coil 13 is broadcast so far by a receiving circuit 11, that it can be evaluated by a microprocessor 3.

The microprocessor 3 is comprised principally of a CPU 5, an EEPROM 6 for the storage of the interrogation program, a RAM 7 for operational purposes, and an interface module 4. The interface module 4, together with the interrogation program, runs the interface 1. By means of this interface 1, the distance detector AL is coupled to the personal computer DE. In the case of an already operative version, the interface 1 is a V.24-Interface to a personal computer. In the presented version in Fig. 1, in which the

[German Column No. 7]

electronic subassembly 2 of the distance detector AL is slipped into the data terminal as a functional card, then the interface 1 is designed as an internal bus-interface.

In operation, by means of the capacity chain 9, 10, 12, 13 an alternating magnetic field of a limited active extent is produced, which induces an alternating voltage in the miniature coil 15 of the identification carrier ID. This alternating voltage is converted to the necessary operational voltage in chip 14. The identification carrier ID subsequently transmits the user recognition which is stored therein in binary form. The data are received by the receiving branch 13, 12, 11 of the distance detector AL and processed in the microprocessor 3 and there evaluated. The microprocessor 3 exerts control through the interface 1 over the distance detector DE and releases therein free programmable reactions, which, in accord with the function flow diagram of with Fig. 6 are executed.

Fig. 5 shows an embodiment or the distance detector AL which is an alternative to that shown in Fig. 1. Involved here is a wedge shaped housing 23, in which not only the send and receive coil 13 is located, but also the electronic subassembly 2. The housing 23 is comprised of a medium thick, fiber plate (MDF) and is laid frontally before the keyboard TA of a portable personal computer. A green light-diode 21 on the upper side of the housing 23 denotes the presence of an identification carrier ID in the active zone of the sending and receiving coil 13.

The connection to the personal computer is carried out with the help of a connection cable 22 leading out of the housing 23. The connection cable 22 is connected with one of the serial interfaces of the personal computer.

The functional logic flow chart of Fig. 6 shows the most important functions of the interrogation program contained in the distance detector AL. In the function "No User", then no person has connected into the data processing system DV. The data apparatus (personal computer) DE is, for all purposes, blocked, and none of its applications are active. In the function b), the CPU checks out continually the signal of the receiver 11, determining whether or not an identification carrier ID has entered into the active area of the sending and receiving coil 13. In case an identification carrier ID is detected, then the function c) becomes energized. With reference to a data base, the said carrier ID is placed in the EEPROM 6, or the on the memory medium of the personal computer DE, or yet in the central storage of the data processing system DV. In any case, the carrier ID is checked whether or not this user for this data terminal apparatus is admissible. In case the determination is negative, the apparatus DE is blocked and then continues to wait until a new recognition signal is detected.

In case the recognition is admissible, then release is given to enter function d) wherein the data terminal apparatus is made free for use. The presence of the identification carrier ID in the active area of the send and receive coil 1`3 is continually monitored by the function e). As soon as the approved user vacates the said active zone, then the data terminal apparatus is blocked, in a manner to be described, and again waits upon the detection of a further user recognition. The active zone of a housing 23, or of a corresponding desk pad, or another means of containing the sending and receiving coil 13 extends typically less than 20 cm. In no case is the extent more than one meter.

[German Column No.8]

Under the heading of blockage of the data terminal apparatus which is immediately triggered, is to be understood especially a blocking of the keyboard and/or a blank-out of the screen. These blockages are again lifted when the user returns into the active zone.

After the duration of a specified time (for instance, three minutes) the interrogation program can cut-off the user at the data terminal apparatus (LOGOFF). Where especially security sensitive data terminal apparatuses, registration is executed if the user absents himself for a short moment from the data terminal apparatus and this is placed in blockage. The function "Block the keyboard/blank out the screen" can also be released if a non-authorized user comes into the active zone of the distance detector AL. For this protection, additional sensors are to be installed.

Besides the automatic blocking of the data terminal apparatus, naturally, the user is offered the possibility of explicitly ending a conference. The function f) makes the decision as to whether all active applications are ended or whether the automatic blockage function should remain unreleased. Further blocking functions or reactions are programmable, for instance programmed through the interface 1 of the data terminal apparatus.

CLAIMS

Claimed is:

1. A system for the authorization of the user of a data terminal apparatus in which the user bears with him an identification carrier, which, within a prespecified distance can be touch-free interrogated and said carrier is made difficult to lose, and by which system a distance detector, which is installed proximal to the data terminal apparatus and by means of a connection cable is in electrical communication with the data terminal apparatus, detects a personal user recognition signal from the said identification carrier within the prespecified distance,
therein characterized, in that a registration apparatus (SG) at a specified time (for instance daily) programmably enters a new personal user recognition into the identification carrier (ID) and likewise into the data processing system (DV),
therein characterized, in that the identification carrier, which is difficult to lose, is placed on the wrist of the user,

therein characterized, in that the prespecified distance between the identification carrier (ID) and the distance detector (AL) and thereby also the distance between the identification carrier (ID) and the data terminal apparatus (DE) is less then 1 meter **and therein characterized**, in that not only the interrogation but also the programming of the personal user recognition is transmitted by a magnetic, alternating field.

2. An authorization system in accord with Claim 1, therein characterized, in that the employed data terminal apparatus is a personal computer.

3. An authorization system in accord with Claim 1, therein characterized, in that the employed data terminal apparatus is a work station.

4. An authorization system in accord with Claim 1, therein characterized, in that the employed data terminal apparatus is a personal computer.

5. An authorization system in accord with Claims 1 to 4, therein characterized, in that the registration apparatus (SG) transmits the generated user recognition to the central data base of the data processing systems (DV).

[German Column No.9]

6. An authorization system in accord with Claims 1 to 4, therein characterized, in that the registration apparatus (SG) is combined with the distance detector (AL) and the user recognition produced thereby is transmitted to the data base in the said distance detector (AL).

7. *[Omitted in original text.]*

8. An authorization system in accord with one of the foregoing Claims, therein characterized, in that the prespecified distance between the identification carrier (ID) on the one hand and the distance detector (AL) on the other — i.e. the data terminal apparatus (DE) — is less than 20 cm.

9. An authorization system in accord with Claims 1 to 8, therein characterized, in that the data terminal apparatus (DE) is immediately blocked, when the identification carrier (ID) leaves the predetermined distance from the active zone.

10. An authorization system in accord with Claims 1 to 9, therein characterized, in that the input keyboard (TA) is blocked.

11. An authorization system in accord with Claim 9, therein characterized, in that a screen of the data terminal apparatus (DE) is made blank or a printer of the data terminal apparatus is blocked.

12. An authorization system in accord with Claim 9, therein characterized, in that the data terminal apparatus (DE) signs off the user after the expiration of a specified interval of time on the data processing system (DV).

13. A system for the authorization, with which a user of a data processing system who is located proximal to a data terminal apparatus is touch-free authenticated, characterized by:

- an identification carrier (ID), which is comprised of a chip (14) and a miniature coil (15),
- a distance detector (AL), with which an electronic subassembly (2) is connected by a connection cable (12) to a sending and receiving coil,

- and a registration apparatus (SG) for the programming of the identification carrier (ID), which registration apparatus (SG) is centrally, or by means of the data terminal apparatus (DE), is connected to the data processing system (DV).

14. A system in accord with Claim 13, therein characterized, in that the identification carrier (ID) is fastened to an arm band (16).

15. A system in accord with Claim 14, therein characterized, in that the fastening is carried out by a plastic ring (17),

16. A system in accord with Claim 14, therein characterized, in that the fastening is effected by a non-magnetic clip.

17. A system in accord with Claim 13, therein characterized, in that the identification carrier (ID) is inset into an armband (20).

18. A system in accord with Claim 17, therein characterized, in that the arm band (20) possesses a closure means (19) wherein by the opening of which the recognition in the identification carrier is lost.

19. A system in accord with Claim 13, therein characterized, in that the identification carrier (ID) is built into the housing of a wristwatch.

[German Column No. 10]

20. A system in accord with Claim 13, therein characterized, in that the identification carrier (ID) is installed in a finger ring.

21. A system in accord with Claims 13 to 20, therein characterized, in that the distance detector (AL) is protected within a housing (23), which contains an electronic subassembly (2) and a send and receive coil (13) and is designed as a wedge shaped work-desk pad.

22. A system in accord with Claim 21, therein characterized, in that the housing (23) carries a light diode (21) which shows the full authenticity of the user.

23. A system in accord with Claims 13 to 20, therein characterized, in that the sending and the receiving coil 13 of the distance detector (AL) is inlaid in a work-desk equipment base and further characterized in that the electronic subassembly (2) of the distance detector (AL) is placed upon a card which can be inserted into the data terminal apparatus (DE)

24. A system in accord with the Claims 13 to 23, therein characterized, in that an additional sensor (ZS) is provided, which is sensitized for the approach of an identification carrier (ID) on a further input means, in particular a so-called mouse.

25. A system in accord with one of the Claims 13 to 24, therein characterized, in that further sensors are provided, which register the approach of non-approved persons.

26. A system in accord with Claims 13 to 25, therein characterized, in that the electronic subassembly (2) of the distance detector (AL) is connected through a serial interface to the data terminal apparatus (DE).

27. A system in accord with claims 13 to 25, therein characterized, in that the electronic subassembly (2) of the distance detector (AL) is connected through an internal interface to the data bus of the data terminal apparatus (DE).

[This concludes DE 40 15 482]

Fig. 1: Main Components

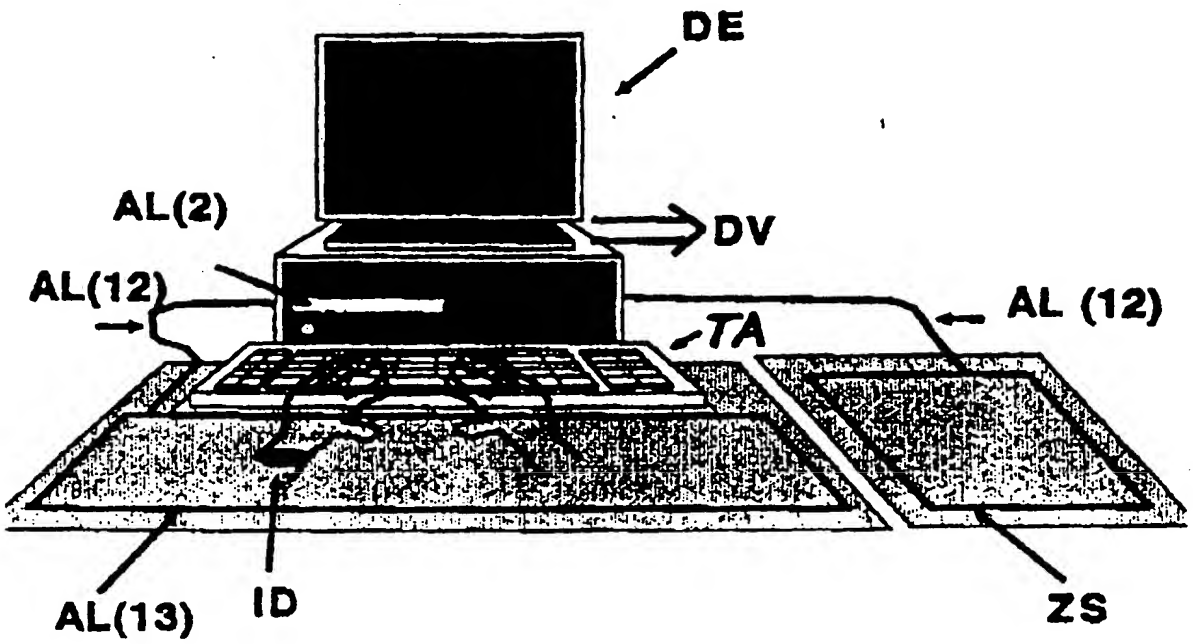


Fig. 2: Block diagram of the ID carrier

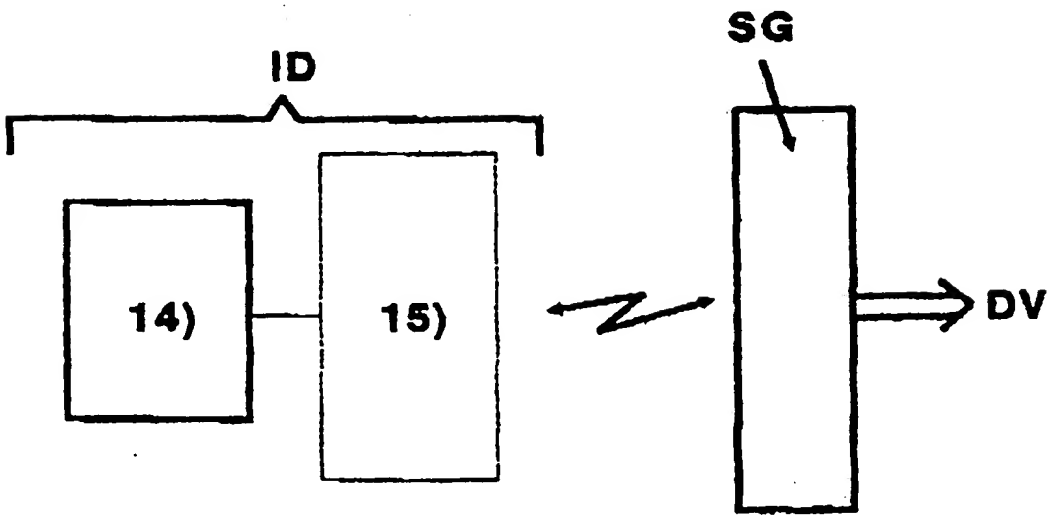


Fig. 3: Forms of the ID carrier

Fig. 3.1: Fastening on an armband

Fig. 3.2: Integrated in a wristwatch

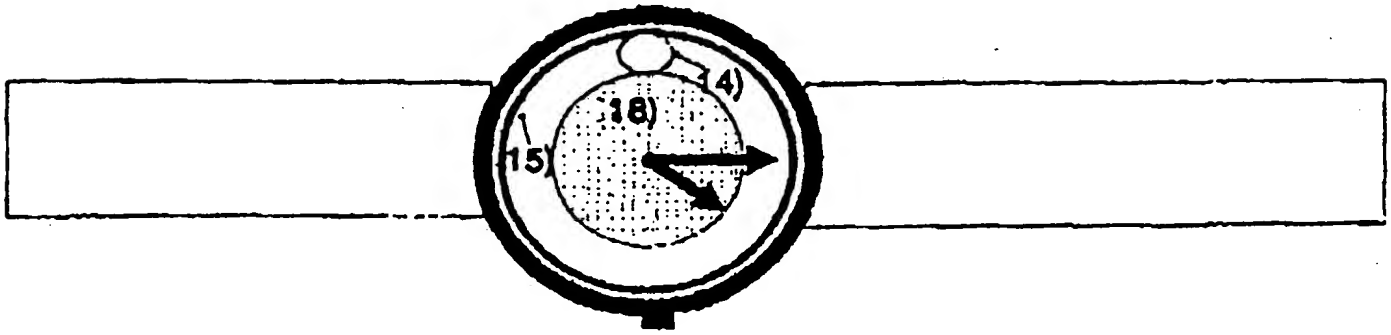
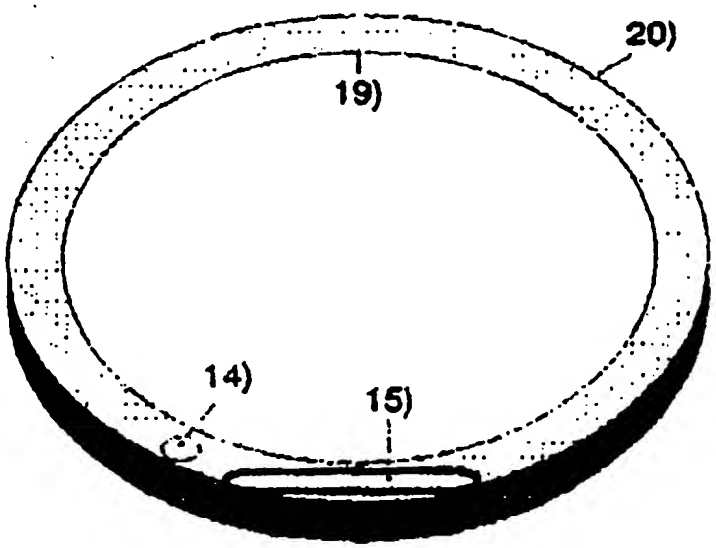


Fig. 3.3: Integrated in an armband



Nummer: DE 40 15 482 C1
Int. Cl.⁵: G 06 F 12/14
Veröffentlichungstag: 26. Juli 1991

Fig. 4: Block circuit diagram of the "Distance Detector"

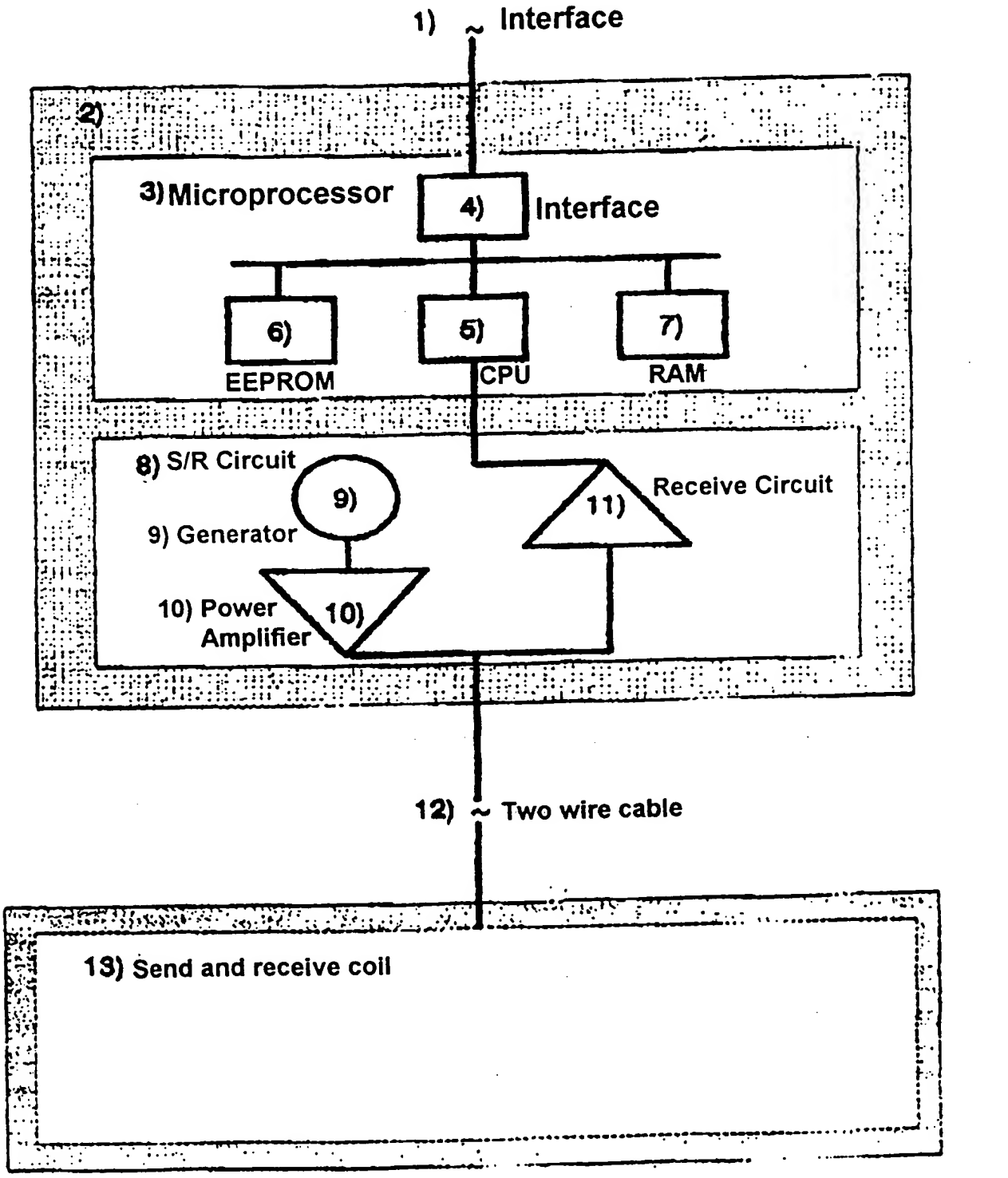


Fig. 5: Housing for "Distance Detector"

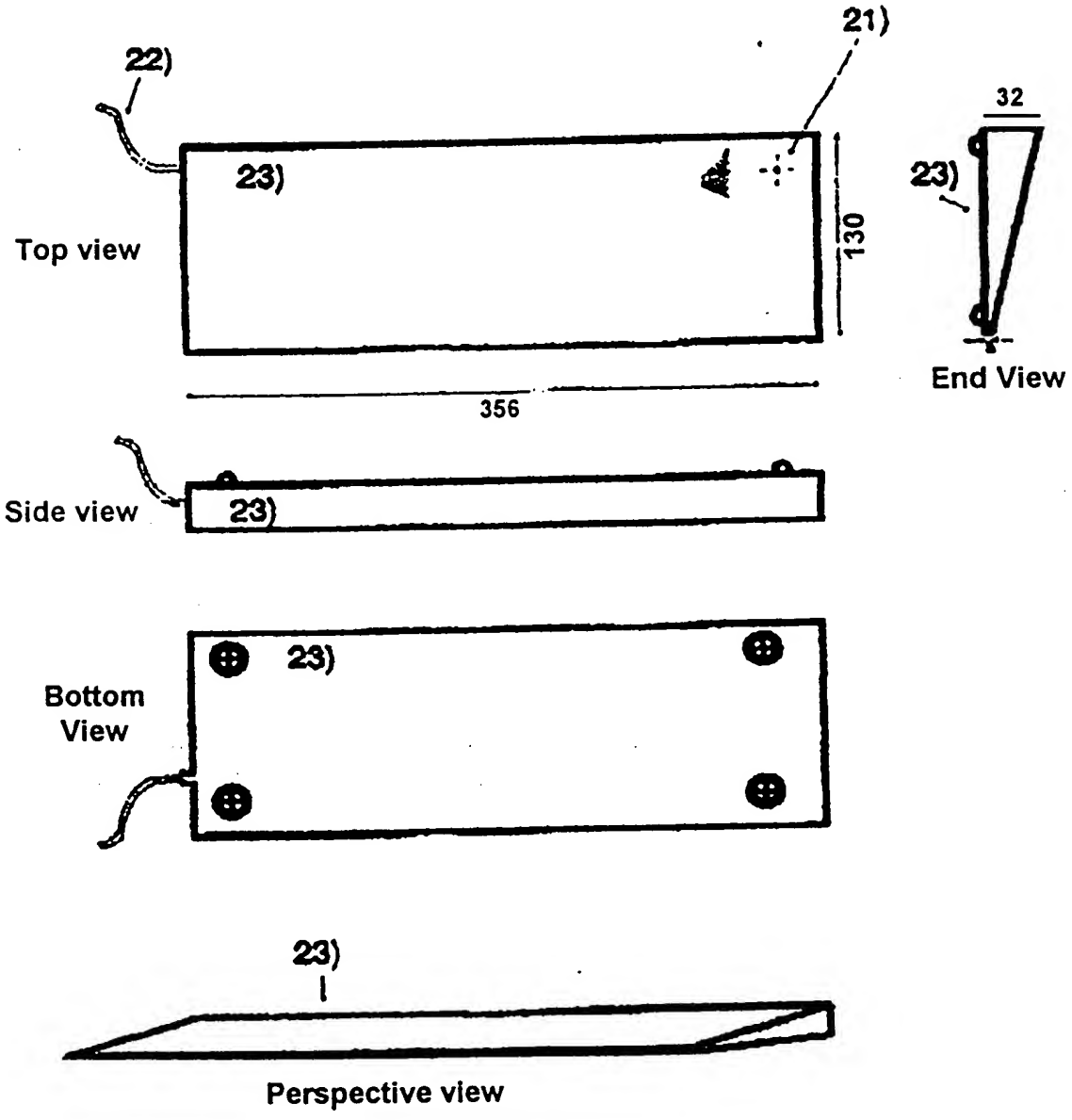
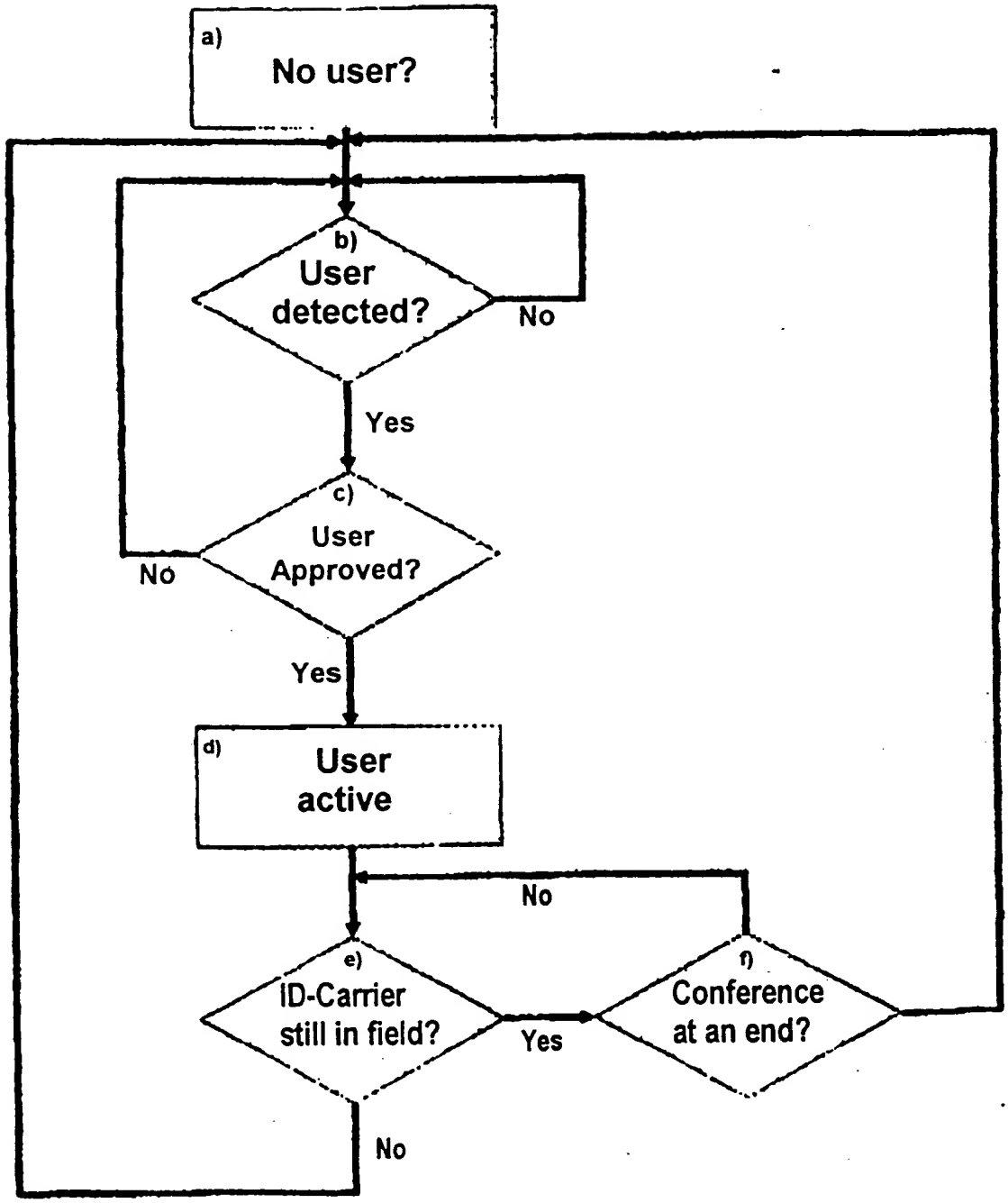


Fig. 6: Functional logic flow diagram



BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.